Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of detecting a malware comprising the steps of:

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

in response to the intercepting, waiting a time interval between the intercepting and scanning the file for a malware; and

scanning the file for the malware, after waiting the time interval [[.]] ;

wherein the process is associated with an application program and wherein the file access operation is a file write operation.

2. (cancelled)

3. (cancelled)

4. (Original) The method of claim 1, wherein the file has a specified file type.

5. (Original) The method of claim 1, wherein the time interval is predefined.

6. (Original) The method of claim 1, wherein the time interval is user-defined.

7. (Currently Amended) The method of claim 1, wherein the time interval is based on a file type of the file.

8. (Original) The method of claim 1, wherein the time interval is based on the process.

9. (Original) The method of claim 1, wherein the malware is a computer virus.

10. (Original) The method of claim 1, wherein the malware is a computer worm.

11. (Original) The method of claim 1, wherein the malware is a Trojan horse program.

12. (Original) The method of claim 1, further comprising the step of:

allowing the intercepted file access operation of the process to a file to complete.

13. (Original) The method of claim 12, further comprising the step of:

allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.

14. (Currently Amended) A system for detecting a malware comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

in response to the intercepting, waiting a time interval between the intercepting and scanning the file for a malware; and

scanning the file for the malware, after waiting the time interval [[.]] ;

wherein the process is associated with an application program and wherein the file access operation is a file write operation.

15. (cancelled)

16. (cancelled)

17. (Original) The system of claim 14, wherein the file has a specified file type.

18. (Original) The system of claim 14, wherein the time interval is predefined.

19. (Original) The system of claim 14, wherein the time interval is user-defined.

20. (Currently Amended) The system of claim 14, wherein the time interval is based on a file type of the file.

21. (Original) The system of claim 14, wherein the time interval is based on the process.

22. (Original) The system of claim 14, wherein the malware is a computer virus.

23. (Original) The system of claim 14, wherein the malware is a computer worm.

24. (Original) The system of claim 14, wherein the malware is a Trojan horse program.

25. (Original) The system of claim 14, further comprising the step of:
allowing the intercepted file access operation of the process to a file to complete.

26. (Original) The method of claim 25, further comprising the step of:
allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.

27. (Currently Amended) A computer program product for detecting a malware comprising:
a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

in response to the intercepting, waiting a time interval between the intercepting and scanning the file for a malware; and

scanning the file for the a malware, after waiting the time interval [[.]] ;

wherein the process is associated with an application program and wherein the file access operation is a file write operation.

28. (cancelled)

29. (cancelled)

30. (Original) The computer program product of claim 27, wherein the file has a specified file type.

31. (Original) The computer program product of claim 27, wherein the time interval is predefined.

32. (Original) The computer program product of claim 27, wherein the time interval is user-defined.

33. (Currently Amended) The computer program product of claim 27, wherein the time interval is based on a file type of the file.

34. (Original) The computer program product of claim 27, wherein the time interval is based on the process.

35. (Original) The computer program product of claim 27, wherein the malware is a computer virus.

36. (Original) The computer program product of claim 27, wherein the malware is a computer worm.

37. (Original) The computer program product of claim 27, wherein the malware is a Trojan horse program.

38. (Original) The computer program product of claim 27, further comprising the step of:

allowing the intercepted file access operation of the process to a file to complete.

39. (Original) The computer program product of claim 38, further comprising the step of:

allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.

40. (New) The method of claim 1, wherein at least a portion of the file access operations are completed before the scanning.

41. (New) The method of claim 1, wherein at least a portion of the file access operations are completed during the scanning.

42. (New) The method of claim 1, wherein the file access operations that occur on the file after the intercepting of a file write operation are completed before the scanning.

43. (New) The method of claim 1, wherein the file access operations that occur on the file after the intercepting of a file write operation are completed during the scanning.

44. (New) The method of claim 1, wherein, if a set of the file access operations lasts less than the time interval, only a last file access operation of the set is scanned.

45. (New) The method of claim 1, wherein only a sample of a set of the file access operations is scanned.

46. (New) The method of claim 1, wherein a final version of the file is scanned, after all of the file access operations of a set are complete.

47. (New) The method of claim 1, wherein the time interval is longer than at least one of an open cycle, a write cycle, and a close cycle associated with the file access operations.

48. (New) The method of claim 1, wherein the time interval is initiated after interception of a first file access operation such that, during the time interval, multiple subsequent file access operations are completed without the scanning, after which the file is scanned.